Cardinality - Size

We have already defined the **cardinality** of a set to be its **size**.

For finite sets, this just means the number of elements and in principal we know how to count.

But explicitly counting only works on sets that I can explicitly write out, and what if I can't? what strategies are there for proving things about the number of elements in sets?

And what can we say about sets which are not finite?

Cardinality - Reinterpretting Size

- Imagine there is an injective map $f : A \to B$, what does this suggest about

$$|A| \qquad \text{vs} \qquad |B|$$

- Imagine there is a surjective map $f : A \to B$, what does this suggest about

$$|A| \qquad \text{vs} \qquad |B|$$

- Imagine there is a bijective map $f : A \to B$, what does this suggest about

$$|A| \qquad \text{vs} \qquad |B|$$

How do we count the items in a set

How do we show that there are at least n elements in the set X?
If I can give a list of $x_1, \ldots, x_n$ of n of them... and show they do not repeat

How do we show there are at most n elements in the set X?
If I can give a list of $x_1, \ldots, x_n$ of n of them (possibly with repeats)... and convince you it includes all of them

How do we show there are exactly n elements in the set X?
If I can give a list of $x_1, \ldots, x_n$ of n of them and convince you it includes all of them with no repeats
An indexed list $x_1, \ldots, x_n$ is just a function $f : \{1, \ldots, n\} \to X$
Not repeating is injective, all of them is surjective, both is bijective.

Cardinality - informal

We wish to define the **cardinality** of a set A, that is $|A|$.
We could define

$$|A| \leq |B|$$

if there exists an injection from $f : A \to B$.

We could also define

$$|A| \geq |B|$$

if there exists an surjection from $f : A \to B$.

Which is better? Do these ideas agree? If the sets are finite they definitely agree, but otherwise:

Theorem (only if direction uses Axiom of Choice)
if A is nonempty we have:

there exists an injection from $f : A \to B$.

if and only if

there exists an surjection from $f : B \to A$.

Cardinality - informal

We could also say:

$$|A| = |B|$$

If we have $|A| \leq |B|$ and $|B| \leq |A|$. (this of course requires us to first agree on the definition of $\leq$. But as we say above this doesn't really matter.)

So

$$|A| = |B|$$

If there exists an injection $f : A \to B$ and an injection $g : B \to A$.

Or we could have said:

$$|A| = |B|$$

if there exists a bijection between $f : A \to B$.

Do these two definitions agree?

Theorem(Shrőder-Bernstein Theorem)
There exists a bijection from $f : A \to B$ if and only if there exists injections $g : A \to B$ and $h : B \to A$.
That is, both hypothetical definitions of $|A| = |B|$ agree!

Cardinality - Formal

Definition: We say that $|A| = |B|$, that is they have the same **Cardinality** if their exists a bijection from A to B.

Theorem
Cardinality defines an equivalence relation on the collection of all sets.

Definition: We say that $|A| \leq |B|$ or $|B| \geq |A|$, that is that A has a smaller **Cardinality** than B, if there exists an injection from A to B.

Theorem(proof uses Axiom of Choice)
If A and B are sets, then either $|A| \leq |B|$ or $|B| \leq |A|$.
(so $|A| < |B|$ or $|A| = |B|$ or $|A| > |B|$!)

Definition: We say that $|A| = n$ if there exists a bijection $A \to \{1, 2, \ldots, n-1, n\}$.

Theorem
If sets A and B are finite and both have exactly n elements then every injection $f : A \to B$ is a bijection.

Of course the map $\mathrm{inc} : \mathbb{N} \to \mathbb{N}$ given by $\mathrm{inc}(n) = n + 1$ is not a bijection.

How are these definitions useful?

We can prove things without the phrase:

just look at it, it is obvious.

Theorem

If $|A| = n$ and $|B| = m$ then $|A \times B| = nm$.

Sketch of Proof

Assume $m \neq 0$ (the case $m = 0$ uses a different proof)
Step 1: There exists bijections $f : A \to \{1, 2, \ldots, n\}$ and $g : B \to \{1, 2, \ldots, m\}$.
We can show (you can!!) that the map $h : A \times B \to \{1, 2, \ldots, n\} \times \{1, 2, \ldots, m\}$ given by $h(a, b) = (f(a), g(b))$ is a bijection. (This is a general property of maps and cartesian products)
Step 2: We now define a function from $i : \{1, 2, \ldots, n\} \times \{1, 2, \ldots, m\} \to \{1, 2, \ldots, mn\}$ by:

$$i(a, b) = (a - 1)m + b$$

Step 3: We must show it is a function, That is, the output values are all in the codomain!
Indeed $0 \leq (a - 1) \leq n - 1$ so $0 \leq (a - 1)m \leq mn - m$, now using that $1 \leq b \leq m$ we obtain $1 \leq (a - 1)m + b \leq mn$.

Step 4: We then must show it is injective. Let (a_1, b_1), (a_2, b_2) be arbirary and assume $i(a_1, b_1) = i(a_2, b_2)$
So $(a_1 - 1)m + b_1 = (a_2 - 1)m + b_2$ thus b_1 and b_2 are congruent modulo m,
(why does this imply they are equal?)
Once $b_1 = b_2$ that $a_1 = a_2$ is an easy check (by solving the equation using that $m \neq 0$).

Step 5: We must show that it is surjective.
Pick $y \in \{1, \ldots, mn\}$ and use long division to write $y = qm + r$. Then, if $r \neq 0$ set $a = q + 1$ (noting it is in the right range because if $q = m$ then $r = 0$) and $b = r$ otherwise if $r = 0$ set $a = q$ (noting that if $r = 0$ that $q \neq 0$) and $b = m$. (Now you can now explain why $i(a, b) = y$).

Step 6: We now have that $i \circ f$ is the desired bijection.

Remark

This proof demonstrates one of the great features of Cardinality, we can replace the set we are trying to prove something about by an equivalent one that we can actually describe.

Recall I mentioned this was one of the great things about equivalence relations.

What can remain very hard about this is picking the correct representative of an equivalence class that allows you to write a proof
(For example, that proof is actually cleaner if we use $\{0, \ldots, n-1\}$...)

This proof demonstrates one of the annoying features of Cardinality, defining explicit bijections can be a bit of a mess, and often involves clever constructions.
In this course we will not have you need to come up with elaborate constructions like these.

Theorem
If $|A| = n$ then $|\mathcal{P}(A)| = 2^n$.

Sketch of Proof
We will proceed by induction on n. Let $P(n)$ be the assertion *If* $|A| = n$ *then* $|\mathcal{P}(A)| = 2^n$.
We shall use two base cases
The case $n = 0$ we have $A = \emptyset$ and $\mathcal{P}(A) = \{\emptyset\}$, which proves $P(0)$.
The case $n = 1$ we have $A = \{x\}$ and $\mathcal{P}(A) = \{\emptyset, \{x\}\}$, which proves $P(0)$.

For the inductive case, suppose $n > 0$ and assume $P(n-1)$
As $n > 0$ then there exists an element $x \in A$.
Define $B = A \setminus \{x\}$. Then $|B| = n - 1$. (you can actually prove that too!) so because we know $P(n-1)$ we know $|\mathcal{P}(B)| = 2^{n-1}$.
Define a map $F : \mathcal{P}(A) \to \mathcal{P}(B) \times \mathcal{P}(\{x\})$ by:

$$F(U) = (U \cap B, U \cap \{x\})$$

We define a map $G : \mathcal{P}(B) \times \mathcal{P}(\{x\}) \to \mathcal{P}(A)$ by

$$G(U, V) = U \cup V$$

One should make it clear that these are functions!
Now prove F and G are inverses, this comes down to a few proofs of set equality, for example:

$$U = (U \cap (A \setminus \{x\})) \cup (U \cap \{x\})$$

We conclude that we have a bijection, and by our previous theorem we get:

$$|\mathcal{P}(A)| = |\mathcal{P}(B) \times \mathcal{P}(\{x\})| = |\mathcal{P}(B)||\mathcal{P}(\{x\})| = 2^{n-1}2 = 2^n$$

which proves the inductive case, and so the result now follows by induction.

Why did I prove $n = 1$ as a base case?

Remark

Both of these proofs demonstrate one of the more challenging things about proofs with Cardinality.
Many of them eventually require constructing explicit maps, figuring out what map to use can be hard.

Other theorems about sizes.

We can also count the number of functions between sets A and B.

Theorem

If $|A| = n$ and $|B| = m$ then

$$|\{f : A \to B\}| = m^n$$

Proof by induction on n.

We can also prove the following

Theorem

If A, B, C are sets, and $A \cap B = \emptyset$ then there is a bijection between:

$$\{f : A \to C\} \times \{g : B \to C\} \quad \text{and} \quad \{h : (A \cup B) \to C\}$$

and hence:

$$|\{f : (A \cup B) \to C\}| = |\{f : A \to C\} \times \{f : B \to C\}| = |\{f : A \to C\}||\{f : B \to C\}|$$

$$(f, g) \mapsto h(x) = \begin{cases} f(x) & x \in A \\ g(x) & x \in B \end{cases}$$

So one key thing cardinality gives us, is a way to reason and write proofs about size:

- If $A \cap B = \emptyset$ then $|A \cup B| = |A| + |B|$.
- $|A \times B| = |A||B|$.
- $|\mathcal{P}(A)| = 2^{|A|}$.
- $|\{f : A \to B\}| = |B|^{|A|}$.
- The combining theorems on last few slides tells us

$$|C|^{|A \cup B|} = |C|^{|A|+|B|} = |C|^{|A|}|C|^{|B|}$$

which is clear enough for finite sets, but now also makes sense for infinite sets.

What else can Cardinality do: The Pigeon Hole Principal

Theorem
If $f : A \to B$ is a function, and if $|A| > |B|$, then there exists $b \in B$ such that $|f^{-1}(\{b\})| > 1$.

If I am trying to put 10 pigeons in 9 holes... then at least 2 pigeons will be sharing.

Or more generally we have the theorem:
Theorem
If $f : A \to B$ is a function, and if $|A| > |B \times C|$, then there exists $b \in B$ such that $|f^{-1}(\{b\})| > |C|$.

If I have 100 pigeions and 9 holes... then there is a hole with at least 12 pigeons.

Both of these work with infinite sets... but one needs to have a strict $>$!!

Both of these can be proven using the definition of cardinality.
By contradiction if for all $b \in B$ we have $|f^{-1}(\{b\})| \leq |C|$ then for all b we have injective functions $g_b : f^{-1}(\{b\}) \to C$, define a function $h : A \to B \times C$ by

$$h(a) = (f(a), g_{f(a)}(a))$$

Explain why this describes a well defined function! then why it is injective.

Dealing with infinite sets - (Theorems about $\mathbb{N}$)

The pigeon hole principal applies to infinite sets, and those ideas about relative sizes do to, so it would be nice to be able to be confidently able to say if $|A| < |B|$ for infinite sets.

Theorem
Every infinite subset A of $\mathbb{N}$ has $|A| = |\mathbb{N}|$.
Proof Idea
Define an injective function $s : \mathbb{N} \to A$ by

$$s(k) = k\text{-th smallest element of } A$$

use induction to prove this is a function! (This whole thing is a well-ordering argument)

Theorem (requires some axiom like AOC)
The natural numbers are the smallest infinite set.

Theorem
There is a bijection $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ and so $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$
for example:

$$f(a, b) = (a + 1)(b + 1) + (b + 1)b/2 + a(a - 1)/2 - 1$$

Dealing with infinite sets (Theorems about $\mathbb{R}$)

Theorem
There is a bijection $\mathbb{R} \to (-1, 1)$. Consequently there is a bijection $\mathbb{R} \to (a, b)$ whenever $a < b$.
For example

$$f(x) = \frac{2}{\pi}\arctan(x) \qquad g(x) = \frac{b-a}{2}\frac{2}{\pi}\arctan(x) + \frac{b-a}{2}$$

Theorem
There is a bijection $[-1, 1] \to (-1, 1)$. Consequently there is a bijection $[a, b] \to (c, d)$ whenever $a < b$ and $c < d$.
This one is more annoying to describe!!

Theorem
All of

$$\mathbb{R}, \quad (a, b), \quad (a, b], \quad [a, b), \quad [a, b]$$

have the same size!

Cantors Diagonal Argument (comparing $\mathbb{N}$ and $\mathbb{R}$)

Theorem

There is no injective map from $[0,1]$ to $\mathbb{N}$, and so $|\mathbb{N}| < |[0,1]| = |\mathbb{R}|$.

(because there is no bijection, because there is no surjection $\mathbb{N}$ to $[0,1]$)

To see there is no surjection $f : \mathbb{N} \to [0,1]$ write out:

$$
\begin{aligned}
f(0) &= 0.a_{00}\,a_{01}\,a_{02}\,a_{03}\,a_{04}\,a_{05}\,a_{06}\,a_{07}\cdots a_{0n}\cdots\\
f(1) &= 0.a_{10}\,a_{11}\,a_{12}\,a_{13}\,a_{14}\,a_{15}\,a_{16}\,a_{17}\cdots a_{1n}\cdots\\
f(2) &= 0.a_{20}\,a_{21}\,a_{22}\,a_{23}\,a_{24}\,a_{25}\,a_{26}\,a_{27}\cdots a_{2n}\cdots\\
f(3) &= 0.a_{30}\,a_{31}\,a_{32}\,a_{33}\,a_{34}\,a_{35}\,a_{36}\,a_{37}\cdots a_{3n}\cdots\\
f(4) &= 0.a_{40}\,a_{41}\,a_{42}\,a_{43}\,a_{44}\,a_{45}\,a_{46}\,a_{47}\cdots a_{4n}\cdots\\
f(5) &= 0.a_{50}\,a_{51}\,a_{52}\,a_{53}\,a_{54}\,a_{55}\,a_{56}\,a_{57}\cdots a_{5n}\cdots\\
f(5) &= 0.a_{60}\,a_{61}\,a_{62}\,a_{63}\,a_{64}\,a_{65}\,a_{66}\,a_{67}\cdots a_{5n}\cdots\\
&\;\;\vdots \qquad\qquad \vdots\\
f(n) &= 0.a_{n0}\,a_{n1}\,a_{n2}\,a_{n3}\,a_{n4}\,a_{n5}\,a_{n6}\,a_{n7}\cdots a_{nn}\cdots
\end{aligned}
$$

where a_{ij} is the j-th decimal digit of $f(i)$.

If we set $b_i = (9 - a_{ii})$ then the number $0.b_0\,b_1\,b_2\,b_3\,b_4\,b_5\,b_6\cdots$ is not in the list, because it has at least one digit different from everything in the list.

An analogous argument proves:

Theorem

There is no injective map $\mathcal{P}(A) \to A$ and so $A < \mathcal{P}(A) < \mathcal{P}(\mathcal{P}(A)) < \mathcal{P}(\mathcal{P}(\mathcal{P}(A))) < \cdots$

Comparing $\mathcal{P}(\mathbb{N})$ and $\mathbb{R}$

Theorem
There is a bijection $\mathcal{P}(\mathbb{N}) \to [0,1]$ and hence $|\mathcal{P}(N)| = |\mathbb{R}|$.
Proof Idea The formulas below define maps $\mathcal{P}(\mathbb{N}) \to [0,1]$.
The map

$$f(U) = \sum_{x \in U} 2^{-x}$$

is surjective, because every number has a binary expansion.

$$g(U) = \sum_{x \in U} 2^{-2x}$$

is injective, because this gives distinct binary expansions.
Because there is both an injective and surjective map... there must be a bijection, even if this doesn't describe it explicitly.

Countable Sets

We say a set is **finite** if there exists an $n \in \mathbb{N}$ such that $|A| = n$.

We say a set is **countable** if $(A = \emptyset)$ or there exists a surjection $\mathbb{N} \to A$.

We say a set is **countably infinite** if there exists a bijection $\mathbb{N} \to A$.

We say a set is **uncountable** if there exists no surjective map $\mathbb{N} \to A$.

Examples of Countably Infinte Sets

- $\mathbb{N}$ by definition.
- $\mathbb{Z}$.
- $\mathbb{N} \times \mathbb{N}$
- $\mathbb{Z} \times \mathbb{Z}$
- $\mathbb{Q}$
- $\mathbb{Q} \times \mathbb{Z} \times \{1, 2, 3\}$

Theorems about Countably infinite sets that you should know

- If A is an infinte subset of a countably infinte set then A is countably infinite. (AOC).
- If A is countably infinite, and B is countable but not empty then $A \cup B$ and $A \times B$ are countably infinite.
- If A is countably infinite then $\mathcal{P}(A)$ is **uncountable**.
- If A is infinite, and $|B| > 1$ then the functions from A to B are **uncountable**.

Examples of Uncountable Sets

- $\mathbb{R}$
- $\mathcal{P}(\mathbb{N})$.
- Any interval $[a, b]$ where $a < b$.
- The set of functions $\{f : \mathbb{N} \to \mathbb{N}\}$ (this set has cardinality $|\mathbb{R}|$)
- The set of functions $\{f : \mathbb{R} \to \mathbb{R}\}$ (cardinality is $|\mathcal{P}(\mathbb{R})| > |\mathbb{R}|$)
- The set of continuous functions $\{f : \mathbb{R} \to \mathbb{R}\}$ (cardinality is $|\mathbb{R}|$, which is not obvious)
- The set $\mathbb{R} \times \mathbb{R}$ (which has cardinality $|\mathbb{R}|$, which is not obvious but a bit less so)

Theorems about uncountable sets that you should know

- If $A \subset B$ and A is uncountable then B is uncountable.
- if A is uncountable, and B is not empty then $A \cup B$, $A \times B$, and $\mathcal{P}(A)$ are uncountable.
- If A is infinite, and $|B| > 1$ then the functions from A to B are uncountable.

Expectations

Proving things about cardinality can be hard, and we won't expect you to produce any of the serious arguments given here.

You should know the definition of cardinality.

You should know the definition of finite, countable (countably infinite), and uncountable and be able to identify (reasonably simple) examples of each. You do not need to distinguish between $|\mathbb{R}|$ and $|\mathcal{P}(\mathbb{R})|$ as I did on the last slide

You should know the theorems on the previous two slides, and the cardinalities of

$$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, (0,1), \text{any interval in } \mathbb{R}$$

.

The Pigeon hole principal, and Cantor's diagonalization argument (proof that $|\mathbb{N}| < |\mathbb{R}|$ are very powerful proof techniques, but I am not expecting you to reproduce them on the exam.

Examples

$\mathcal{P}([1,2])$
$\mathcal{P}$(set of even numbers).
$\mathbb{Z} \times \mathbb{Z}$.
$\mathbb{Z} \times$ (set of even numbers).
$\mathcal{P}([3,4] \times \mathbb{Z})$.
Rational number whose denominator is 2.
The set of rational numbers whose numerator and denominator have absolute value less than 10.
$\mathcal{P}(\{1,2,3,4,5\} \times \{1,3,5,7\})$.
$\mathbb{Z} \times \mathbb{Q}$
$\mathcal{P}(\mathbb{Z} \times \mathbb{Q})$.
The set of functions from $\mathbb{Q}$ to $\mathbb{Z}$.
$\mathcal{P}(\{1,2,3,4,5\} \times \{1,3,5,7\}) \times \mathcal{P}(\mathbb{Z})$.
$\mathbb{R} \times \mathbb{N} \times \mathbb{R}$.
$\mathbb{R} \times \emptyset$.

Final challenge problem (not testable)

$$|\mathbb{N}| \leq |\{X \in \mathcal{P}(\mathbb{N}) \mid X \text{ is finite}\}| \leq |\mathcal{P}(\mathbb{N})|$$

is one of these an equality?
the proof is another clever construction.

There is a bijection from finite subsets of $\mathbb{N}$ to $\mathbb{N}$ given by:

$$U \mapsto \sum_{x \in U} 2^x$$

If U is a finite set, this is a finite sum.
This process gives the number whose binary digits are decided by the elements of U.
The inverse is:

$$x \mapsto \{u \in \mathbb{N} \mid u\text{th}\text{binary digit of } x \text{ is } 1\}$$

A consequence is that most subsets of the natural numbers are infinite.